

On the security of arbitrated quantum signature schemes

Qin Li,^{1,*} Chengqing Li,^{1,2} Zhonghua Wen,¹ Weizhong Zhao,¹ and W. H. Chan³

¹*College of Information Engineering, Xiangtan University, Xiangtan 411105, China*

²*Department of Electronic and Information Engineering,
The Hong Kong Polytechnic University, Hong Kong*

³*Department of Mathematics and Information Technology,
The Hong Kong Institute of Education, Hong Kong*

Due to potential capability of providing unconditional security, arbitrated quantum signature (AQS) schemes, whose implementation depends on the participation of a trusted third party, received intense attention in the past decade. Recently, some typical AQS schemes were cryptanalyzed and improved. In this paper, we analyze security property of some AQS schemes and show that all the previous AQS schemes, no matter original or improved, are still insecure in the sense that the messages and the corresponding signatures can be exchanged among different receivers, allowing the receivers to deny accepting the signature of an appointed message. Some further improvement methods on the AQS schemes are also discussed.

PACS numbers: 03.67.Dd

Digital signature, as an electronic equivalent to hand-written signature in online transactions, is a very important cryptographic primitive and has many different uses. For instance, it can be used to authenticate the identity of the originator, ensure data integrity, and provide non-repudiation service. At present, classical (digital) signature has been widely used in electronic commerce and other related fields. Unfortunately, most existing classical signature schemes whose security depends on the difficulty of solving some hard mathematical problems were threatened by quantum computation [1]. Therefore, researchers turn to investigate its quantum counterpart with the hope that quantum signature can become an alternative to classical signature and provide unconditional security.

Generally, a quantum signature scheme is believed to be unconditionally secure if the following two basic requirements are satisfied even though powerful quantum cheating strategies exist and unlimited computing resources are available: 1) the attacker (or the malicious receiver) cannot forge the signature; 2) disavowal of the signatory and the receiver is impossible. In 2002, unconditionally secure quantum signature was proved to be impossible by Barnum *et al.* [2]. Even the result is disappointing, Zeng and Keitel proposed an arbitrated quantum signature (AQS) scheme with the aid of a trusted third party named arbitrator [3]. Afterwards, Li *et al.* found that the arbitrator is unnecessary to entangle with the other two participants in the AQS scheme presented in Ref. [3] and thus the three-particle entangled GHZ states used in the scheme can be replaced with two-particle entangled Bell states [4]. In addition, the preparation and distribution of Bell states are much easier to be implemented than that of GHZ states with the present-day technologies. So, Li *et al.* proposed a more

efficient AQS scheme using Bell states [4]. Zou *et al.* showed both the two schemes proposed in Ref. [3] and Ref. [4] are insecure since they could be repudiated by the receiver Bob and presented two AQS schemes claimed to fix the secure problem [5]. But Hwang *et al.* pointed out in Ref. [6] that the arbitrator cannot solve the dispute between the signatory Alice and the receiver Bob when Bob claims a failure in the verification phase of the scheme proposed by Zou *et al.* Besides, some other security problems of these typical AQS schemes were also been discovered [7–10].

In this paper, we study security of all the above mentioned AQS schemes [3–5] and find that a common problem existing in the AQS schemes: different receivers can exchange their signed messages and the corresponding signatures arbitrarily, and thus they can deny the acceptance of the signature of an appointed message. The reason why this security problem exist is also analyzed in detail and the two AQS schemes presented by Zou *et al.* [5] are selected as examples to study. In addition, we also discussed some potential improvement methods for enhancing the security of AQS schemes.

The rest of the paper is organized as follows. Section I introduces the AQS scheme with entangled states given in Ref. [5] and analyzes its security. Section II deals with the AQS scheme without entangled states proposed by Zou *et al.* in [5]. Some discussions for improving the security of AQS schemes are given in Sec. III. The last section concludes the paper.

I. SECURITY ANALYSIS OF THE AQS SCHEME WITH ENTANGLED STATES

In this section, we will briefly introduce the AQS scheme with entangled states proposed in Ref. [5], and then present security analysis on it.

*liqin805@163.com

A. The AQS scheme with entangled states

The AQS scheme with entangled states proposed by Zou *et al.* in Ref. [5] involves three participants, namely signatory Alice, receiver Bob, and the arbitrator, and consists of three phases: the initializing phase, the signing phase, and the verifying phase, which are described as follows.

A. The initializing phase

Step I1: The arbitrator shares keys K_A and K_B with Alice and Bob, respectively, through quantum key distribution protocols proposed in Refs. [11, 12], which have been proved to be unconditionally secure [13, 14].

Step I2: Alice generates N Bell states $|\psi\rangle = (|\psi_1\rangle, |\psi_2\rangle, \dots, |\psi_N\rangle)$ with $|\psi_i\rangle = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})$, where the subscripts A and B correspond to Alice and Bob, respectively. Then she distributes one particle of each Bell state to Bob employing a secure and authenticated method [2, 15].

B. The signing phase

Step S1: Alice transforms the message $|P\rangle$ into $|P'\rangle = E_r(|P\rangle)$ according to a randomly chosen number $r \in \{00, 01, 10, 11\}^N$.

Step S2: Alice generates $|S_A\rangle = E_{K_A}(|P'\rangle)$.

Step S3: Alice combines each message state and the Bell state to obtain the three-particle entangled state

$$\begin{aligned} |\phi_i\rangle &= |p'_i\rangle \otimes |\psi_i\rangle \\ &= \frac{1}{2}\{|\phi_{12}^+\rangle_A(\alpha_i|0\rangle_B + \beta_i|1\rangle_B) \\ &\quad + |\phi_{12}^-\rangle_A(\alpha_i|0\rangle_B - \beta_i|1\rangle_B) \\ &\quad + |\psi_{12}^+\rangle_A(\alpha_i|1\rangle_B + \beta_i|0\rangle_B) \\ &\quad + |\psi_{12}^-\rangle_A(\alpha_i|1\rangle_B - \beta_i|0\rangle_B)\}, \end{aligned} \quad (1)$$

where $|\phi_{12}^+\rangle_A$, $|\phi_{12}^-\rangle_A$, $|\psi_{12}^+\rangle_A$, and $|\psi_{12}^-\rangle_A$ represent the four Bell states respectively [16].

Step S4: Alice implements a Bell measurement on each $|\phi_i\rangle$ and obtains $M_A = (M_A^1, M_A^2, \dots, M_A^N)$, where M_A^i represents one of the four Bell states.

Step S5: Alice transmits the signature $|S\rangle = (|P'\rangle, |S_A\rangle, |M_A\rangle)$ to Bob.

C. The verifying phase

Step V1: Bob encrypts $|P'\rangle$ and $|S_A\rangle$ using the key K_B and sends the resultant outcome $|Y_B\rangle = E_{K_B}(|P'\rangle, |S_A\rangle)$ to the arbitrator.

Step V2: The arbitrator decrypts $|Y_B\rangle$ with K_B and gets $|P'\rangle$ and $|S_A\rangle$. Then he encrypts $|P'\rangle$ with K_A and obtains S_T . If $|S_T\rangle = |S_A\rangle$, the arbitrator sets the verification parameter $V = 1$, otherwise sets $V = 0$.

Step V3: The arbitrator obtains $|P'\rangle$ from $|S_T\rangle$ and sends the encrypted results $|Y_T\rangle = E_{K_B}(|P'\rangle, |S_A\rangle, r)$ to Bob.

Step V4: Bob decrypts $|Y_T\rangle$ and obtains $|P'\rangle$, $|S_A\rangle$, and r . If $r = 0$, Bob rejects the signature, otherwise Bob makes further verification.

Step V5: According to Alice's measurement outcomes M_A and Eq. (1), Bob obtains $|P'_B\rangle$ via teleportation. If $|P'_B\rangle \neq |P'\rangle$, Bob rejects the signature, else informs Alice to publish r .

Step V6: Alice announces r through the public board.

Step V7: Bob recovers $|P\rangle$ from $|P'\rangle$ according to r and takes $(|S_A\rangle, r)$ as the final signature of the message $|P\rangle$.

B. Security analysis

Hwang *et al.* presented the deniability dilemma in the above AQS scheme [6]. They found the arbitrator cannot solve the dispute if Bob claims $|P'_B\rangle \neq |P'\rangle$ in Step V5 since the following three cases may occur: 1) Bob told a lie; 2) Alice sent a incorrect information to Bob; and 3) Eve disturbed the communication. However, if Bob made such an allegation, the verification process cannot be completed and a new signature task should be started. So, here we show that the receiver Bob can repudiate the acceptance of a signature related to a given message after finishing the verification process successfully.

First let Alice sign the message $|P\rangle_B$ for Bob and the message $|P\rangle_C$ for Charlie. Actually, $|P\rangle_B$ is favorable to Charlie, and $|P\rangle_C$ is beneficial to Bob. Then Bob and Charlie can be shown to exchange their messages and the corresponding signatures by using the following method. In step I2, after Alice distributes particles of Bell states to Bob and Charlie, Bob and Charlie exchange the particles they get. Similarly, after step S5, Bob sends the qubit string $|S\rangle_B = (|P'\rangle_B, |S_A\rangle_B, |M_A\rangle_B)$ to Charlie and Charlie returns $|S\rangle_C = (|P'\rangle_C, |S_A\rangle_C, |M_A\rangle_C)$ to Bob. Then Bob can verify the validity of the signature $|S_A\rangle_C$ for the message $|P\rangle_C$ with the help of the arbitrator, and Charlie can check whether $|S_A\rangle_B$ is the signature of $|P\rangle_B$ with the aid of the arbitrator. Obviously, if Alice's signatures are valid, Bob and Charlie can finish the verification processes successfully. After that, Bob gets Alice's signature for the message $|P\rangle_C$ and Charlie obtains Alice's signature related to the message $|P\rangle_B$. Therefore, even if there are disagreements between Alice and Bob or between Alice and Charlie afterwards, Bob still can deny accepting the signature $|S_A\rangle_B$ of the message $|P\rangle_B$, and Charlie also can disavow the acceptance of the signature $|S_A\rangle_C$ related to the message $|P\rangle_C$. Furthermore, the arbitrator is not able to settle the dispute since they passed the verification processes.

II. SECURITY ANALYSIS OF THE AQS SCHEME WITHOUT ENTANGLED STATES

This section reviews the AQS scheme without entangled states proposed by Zou *et al.* in Ref. [5], and then analyzes the security of the scheme.

A. The AQS scheme without entangled states

The AQS scheme without entangled states also involves three participants, namely signatory Alice, receiver Bob, and the arbitrator, and consists of the following three phases.

A. The initializing phase

Step I1: The arbitrator shares keys K_A and K_B with Alice and Bob, respectively. In addition, Alice and Bob shares the key K_{AB} .

B. The signing phase

Step S1: Alice chooses a random number $r \in \{0, 1\}^{2N}$ and computes $|P'\rangle = E_r(|P\rangle)$ and $|R_{AB}\rangle = M_{K_{AB}}(|P'\rangle)$.

Step S2: Alice generates $|S_A\rangle = E_{K_A}(|P'\rangle)$.

Step S3: Alice generates the signature $|S\rangle = E_{K_{AB}}(|P'\rangle, |R_{AB}\rangle, |S_A\rangle)$ and transmits it to Bob.

C. The verifying phase

Step V1: Bob obtains $|P'\rangle$, $|R_{AB}\rangle$, and $|S_A\rangle$ by decrypting $|S\rangle$ with the key K_{AB} . Then he generates $|Y_B\rangle = E_{K_B}(|P'\rangle, |S_A\rangle)$ and sends it to the arbitrator.

Step V2: The arbitrator decrypts $|Y_B\rangle$ with K_B and gets $|P'\rangle$ and $|S_A\rangle$.

Step V3: The arbitrator obtains $|P'_T\rangle$ from $|S_A\rangle$ and compares it with $|P'\rangle$. If $|P'_T\rangle = |P'\rangle$, he sets the verification parameter $V_T = 1$, else sets $V_T = 0$. The arbitrator announces the value of V_T via the public board. If $V_T = 1$, he reproduces Y_B and resends it to Bob.

Step V4: If $V_T = 0$, Bob rejects the signature, otherwise Bob decrypts $|Y_B\rangle$ and obtains $|P'\rangle$ and $|S_A\rangle$. Then he computes $|P'_B\rangle = M_{K_{AB}}^{-1}(|R_{AB}\rangle)$ and compares it with $|P'\rangle$. If $|P'_B\rangle = |P'\rangle$, he sets the verification parameter $V_B = 1$, else sets $V_B = 0$. Bob announces the value of V_B via the public board.

Step V5: If $V_B = 0$, Alice and the arbitrator abort the scheme, otherwise Alice announces r through the public board.

Step V6: Bob recovers $|P\rangle$ from $|P'\rangle$ by r and takes $(|S_A\rangle, r)$ as Alice's final signature of the message $|P\rangle$.

B. Security analysis

In this subsection, we show that the arbitrator also cannot solve the disagreements between signatory and receiver for the AQS scheme without entangled states if the following case happens.

Suppose Alice intend to sign the message $|P\rangle$ for Bob. Afterwards, Bob finds the message $|P\rangle$ is useless or unfavorable to him but beneficial to Charlie. Then by doing the following steps, Charlie can get the signature for $|P\rangle$ without being detected by Alice.

- First, when Bob receives $|S\rangle = E_{K_{AB}}(|P'\rangle, |R_{AB}\rangle, |S_A\rangle)$ related to the message $|P\rangle$ from Alice after step S3, he decrypts it with the key K_{AB}

and obtains $|P'\rangle$, $|R_{AB}\rangle$, and $|S_A\rangle$. In addition, Bob gets another version of $|P'\rangle$ by decrypting R_{AB} with the key K_{AB} .

- Second, Bob transmits two versions of $|P'\rangle$ and $|S_A\rangle$ to Charlie through an authenticated channel.
- Third, after Charlie has received what Bob sent, he encrypts $|P'\rangle$ and $|S_A\rangle$ with the key K_C shared with the arbitrator to obtain $|Y_C\rangle = E_{K_C}(|P'\rangle, |S_A\rangle)$.
- At last, the encrypted result $|Y_C\rangle$ is sent to the arbitrator.

Apparently, Charlie can implement the verification procedure like a honest receiver and get the signature of $|P\rangle$ if it is a valid one made by Alice. Furthermore, the arbitrator and Alice cannot discover the fact. Therefore, if there are disputes between Alice and Bob, Bob can deny that he has accepted the signature of the message $|P\rangle$, and Charlie can claim the signature of $|P\rangle$ does come from Alice if disagreements between Alice and Charlie exist.

III. POSSIBLE ENHANCEMENTS

In this section, we first analyze two reasons why AQS schemes are easy to suffer deniability dilemma problem, and then propose the corresponding improve methods.

One reason is that the signatory Alice cannot identify the real receiver. In other words, there is no relationship between the signed message and the real receiver. Therefore, different receivers can exchange their messages and the corresponding signatures arbitrarily and thus repudiate accepting signatures for appointed messages. Another reason is that when participants announce random numbers or values of verification parameters, the identities of them and the announcement time are not published together. So, the arbitrator cannot distinguish which opened information is related to a specified message during a certain period.

According to the above analysis, we can take the following three measures to enhance the security of AQS schemes.

- First, the signatory Alice's signature not only includes the message, but also the identity of the receiver. Although the property of receivers' deniability is not always necessary in a signature scheme, it is quite useful in some special circumstances. For instance, suppose Alice sign a contract with Bob for a thousand dollars goods. If Bob can deny that he has accepted the contract with the help of another receiver Charlie and ask Alice to do the same thing again, it is quite unfair for Alice.
- Second, when participants are required to announce random numbers or values of verification parameters, their identities and the announcement time

should be also attached. So the arbitrator and the signatory can distinguish when the verification of signatures related to appointed messages is implemented and who participate in the verification process.

- Third, before the signatory Alice start a signature procedure, she can tell the arbitrator who will be the receiver at first.

IV. CONCLUSION

In this paper, we have shown two typical AQS schemes still suffer the security problem, namely receivers can deny any signature for an appointed message after the AQS procedures have been completed successfully. That is because a signed message is unrelated to a receiver,

which allows different receivers to interchange their messages and the corresponding signatures arbitrarily. In addition, some countermeasures also have been presented to fix such a security problem. Whether these countermeasures can overcome all the security problems discovered in Refs. [7–10] and how to design an AQS scheme which can withstand existing or potential attacks deserve further research.

Acknowledgement

This work is supported by Natural Science Foundation of China (Grant Nos. 61070232, 61100216, and 61105052), Scientific Research Fund of Hunan Provincial Education Department (Grant No. 11B124), and Science Fund of Xiangtan University (Grant No. 2011XZX16).

-
- [1] P. W. Shor, in *Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science* (1994) pp. 124–134.
 - [2] H. Barnum, C. Crepeau, D. Gottesman, A. Smith, and A. Tapp, in *Proceedings of the 43th Annual IEEE Symposium on Foundations of Computer Science* (2002) pp. 449–470.
 - [3] G. H. Zeng and C. H. Keitel, *Physical Review A* **65**, article no. 042312 (2002).
 - [4] Q. Li, W. H. Chan, and D. Y. Long, *Physical Review A* **79**, article no. 054307 (2009).
 - [5] X. F. Zou and D. W. Qiu, *Physical Review A* **82**, article no. 042325 (2010).
 - [6] T. Hwang, Y.-P. Luo, and S.-K. Chong, “Enhancement on “security analysis and improvements of arbitrated quantum signature,” (2011), available at arXiv:quant-ph/1109.1744.
 - [7] S.-K. Chong, Y.-P. Luo, and T. Hwang, “On the “security analysis and improvements of arbitrated quantum signature schemes,” (2011), available at arXiv:quant-ph/1105.1232.
 - [8] F. Gao, S. J. Qin, F. Z. Guo, and Q. Y. Wen, *Physical Review A* **84**, article no. 022344 (2011).
 - [9] J. W. Choi, K. Y. Chang, and D. Hong, *Physical Review A* **84**, article no. 062330 (2011).
 - [10] Z. W. Sun, R. G. Du, B. H. Wang, and D. Y. Long, “Improving the security of arbitrated quantum signature protocols,” (2011), available at arXiv:quant-ph/1107.2459.
 - [11] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (1984) pp. 175–179.
 - [12] A. K. Ekert, *Physical Review Letters* **67**, 661 (1991).
 - [13] H.-K. Lo and H. F. Chau, *Science* **283**, 2050 (1999).
 - [14] P. W. Shor and J. Preskill, *Physical Review Letters* **85**, 441 (2000).
 - [15] M. Curty, D. J. Santos, E. Pérez, and P. García-Fernández, *Physical Review A* **66**, article no. 022301 (2002).
 - [16] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih, *Physical Review Letters* **75**, 4337 (1995).